(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2001147976 A**

(43) Date of publication of application: **29.05.01**

(51) Int. Cl **G06F 17/60**
G06K 17/00
G07F 17/00

(21) Application number: **2000257086**

(22) Date of filing: **05.09.95**

(62) Division of application: **07227843**

(71) Applicant: **CANON INC**

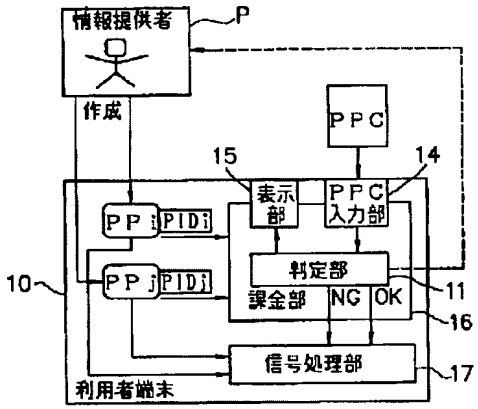
(72) Inventor: **IWAMURA KEIICHI**

(54) CHARGING DEVICE, INFORMATION RECEIVER AND COMMUNICATION SYSTEM

(57) Abstract:

PROBLEM TO BE SOLVED: To easily and suitably manage charging to the information utilization of a user on a multimedia network or the like while protecting the privacy of the user.

SOLUTION: The user inputs the monetary information of cash, prepaid card or IC card to a PPC input part 14 provided on a user terminal 10. Then, on the basis of an amount shown by that monetary information and/or charge information PID added to provided information PP from an information provider P, a discriminating part 11 discriminates whether the provided information PP may be utilized and, corresponding to a signal permitting the utilization, the provided information PP is processed and outputted to the user by a signal processing part 17. The information and the discrimination result on the monetary information are displayed.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－147976
（P2001－147976A）
(43)公開日　平成13年５月29日(2001.5.29)

(51)Int.Cl.'	識別記号	ＦＩ	テーマコード'（参考）
Ｇ０６Ｆ　17/60	３０２	Ｇ０６Ｆ　17/60	３０２Ｅ
	ＺＥＣ		ＺＥＣ
	３３２		３３２
	４０８		４０８
	４１０		４１０Ｅ

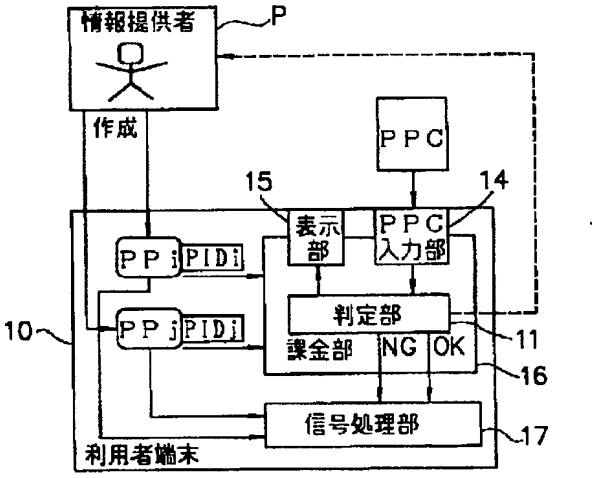
審査請求　未請求　請求項の数17　ＯＬ　（全 13 頁）　最終頁に続く

(21)出願番号　特願2000－257086(P2000－257086)
(62)分割の表示　特願平7－227843の分割
(22)出願日　平成７年９月５日(1995.9.5)

(71)出願人　000001007
キヤノン株式会社
東京都大田区下丸子３丁目30番２号
(72)発明者　岩村　恵市
東京都大田区下丸子３丁目30番２号　キヤノン株式会社内
(74)代理人　100090273
弁理士　國分　孝悦

(54)【発明の名称】　課金装置、情報受信装置及び通信システム

(57)【要約】
【課題】　マルチメディアネットワーク等において利用者の情報利用に対する課金を、管理を容易に行い、かつ利用者のプライバシーを保護しながら適切に行う。
【解決手段】　利用者が利用者端末１０に設けられたＰＰＣ入力部１４に現金、プリペイドカード、ＩＣカード等による金銭情報を入力すると、判定部１１がその金銭情報が示す金額及び／または情報提供者Ｐからの提供情報ＰＰに付加された料金情報ＰＩＤに基づいて提供情報ＰＰの利用可否を判定し、利用を許可する信号に応じて信号処理部１７が提供情報ＰＰを処理して利用者に対して出力する。金銭情報に関する情報及び判定結果は、表示される。



1

【特許請求の範囲】

【請求項１】　記録媒体に記録され、所定の金融機関等にて保証された金額を示す金銭情報が入力される入力手段と、

上記入力手段から入力された金銭情報を判定し、情報提供者から提供される画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の提供情報の利用を許可する許可信号を出力する判定手段と、

上記許可信号に応じて上記提供情報の利用が可能となるように処理する処理手段と、

上記金銭情報に関する情報及び上記判定手段による判定の結果を表示する表示手段とを備えた課金装置。

【請求項２】　上記判定手段は、上記金銭情報と上記提供情報に付加された利用料金情報とに基づいて判定を行うようにした請求項１記載の課金装置。

【請求項３】　上記金銭情報が現金である請求項１記載の課金装置。

【請求項４】　上記記録媒体はＩＣカードである請求項１記載の課金装置。

【請求項５】　情報提供者から提供される画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の提供情報を受信するように成された情報受信装置であって、

所定の金融機関等にて保証された金額を示す金銭情報が入力される入力手段と、

上記入力手段から入力された金銭情報を判定して上記提供情報の利用を許可する許可信号を出力する判定手段と、

上記許可信号に応じて上記提供情報の利用が可能となるように処理する処理手段と、

上記金銭情報に関する情報及び上記判定手段による判定の結果を表示する表示手段とを備えた情報受信装置。

【請求項６】　上記判定手段は、上記金銭情報と上記提供情報に付加された利用料金情報とに基づいて判定を行うようにした請求項５記載の情報受信装置。

【請求項７】　上記金銭情報が現金である請求項５記載の情報受信装置。

【請求項８】　上記金銭情報は記録媒体に記録された情報である請求項５記載の情報受信装置。

【請求項９】　上記提供情報の利用情報を外部に送信する通信手段を備えた請求項５記載の情報受信装置。

【請求項１０】　情報を提供する情報提供者端末装置と、

上記情報提供者端末装置からの画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の提供情報を受信して利用する利用者端末装置と、

所定の金融機関等にて保証された金銭情報を入力するように成され、入力された金銭情報を判定して上記提供情報の利用を許可する許可信号を出力する判定手段と上記許可信号に応じて上記提供情報の利用が可能となるように処理する処理手段と上記金銭情報に関する情報及び上記判定手段による判定の結果を表示する表示手段とを有する課金装置とを備えた通信システム。

2

【請求項１１】　上記判定手段は、上記金銭情報と上記提供情報に付加された利用料金情報とに基づいて判定を行うようにした請求項１０記載の通信システム。

【請求項１２】　上記金銭情報が現金である請求項１０記載の通信システム。

【請求項１３】　上記金銭情報は記録媒体に記録された情報である請求項１０記載の通信システム。

【請求項１４】　上記利用者端末装置に提供情報の利用情報を送信する通信手段を設けた請求項１０記載の通信システム。

【請求項１５】　上記利用情報に応じて上記情報提供者端末装置に料金分配情報を送信する料金分配者端末装置を設けた請求項１４記載の通信システム。

【請求項１６】　上記利用情報に応じて提供情報の利用料金の立替え処理を行う料金立替端末装置を設けた請求項１４記載の通信システム。

【請求項１７】　上記各装置間の通信を暗号通信により行うようにした請求項１０、１４～１６の何れか１項記載の通信システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、動画像データ、静止画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の情報を伝送するマルチメディアネットワーク等で用いられる課金装置、情報受信装置及び通信システムに関し、特に情報の提供とそれに対する課金方式に関するものである。

【０００２】

【従来の技術】近年、幹線通信網における光ファイバネットワークの整備、ケーブルテレビシステムの普及、衛星通信の実用化、ローカルエリアネットワークの普及等に伴い、かかる通信網を利用して様々な情報を提供し、その情報の内容及び量に応じて料金を徴収する、いわゆる情報サービス産業が増大している。このようなサービスにおいては、提供した情報に対する課金を適切に行うことが重要となる。

【０００３】しかしながら、現実では情報の保護は不完全であり、プログラムや映像（音声を含む）情報の不正利用が問題になっている。この不正利用を防ぐために、コピー防止機能を付けたり、コンピュータ等に付与されているハードウェア機番を用い、ソフトウェア自体に上記機番に相当するソフトウェア機番を付与し、プログラム実行時に、２つの機番を照合する等の手法がある。しかし、コピー防止機能はバックアップ等の際不便であるし、機番照合は機番管理や販売に関して不便であり、あまり実用的ではなかった。

【０００４】これに対して、「超流通」というソフトウ

ェア権利者（以後、情報提供者）の権利の保護をめざした概念が森亮一氏によって提案され、特開昭６０－７７２１８号、特開昭６０－１９１３２２号、特開昭６４－６８８３５号、特開平０２－４４４４７号、特開平０４－６４１２９号等の各公報に示された。図１０は特開平０４－６４１２９号公報に示された「超流通」の概念図である。情報提供者Ｐは自分が作成したソフトウェアＰＰｉ（またはＰＰｊ）を利用者端末１０に送る。利用者端末１０はソフトウェアＰＰの利用可否を、ソフトウェアＰＰに付加された固有データＰＩＤｉ（またはＰＩＤｊ）と利用者のユーザＩＤ毎の条件によって判定部１１で判定し、利用可ならば提供情報の利用履歴を記憶部１２に記録し、その履歴に基づいて情報提供者Ｐはその提供情報（ソフトウェアＰＰ）の利用料金等を請求する。１３は以上の各部を含むＳＳＵ（ソフトウェアサービスユニット）である。

【０００５】

【発明が解決しようとする課題】しかしながら上述した「超流通」方式は次のような問題点があった。

（１）「超流通」は情報提供者に許可された利用者であるかどうかをユーザＩＤ等の利用者固有データによって判定し、そのために「超流通」を実現するには、少なくとも利用者固有データの格納手段を設ける必要がある。このような方式では、利用者は予め情報提供者に情報の利用を申し込み、自分のユーザＩＤ等をもらい、一利用者固有データとして登録する必要がある。このような利用申し込みの手続きや、ユーザＩＤのような多くの異なる利用者固有データを管理することは煩雑である。

【０００６】（２）「超流通」は情報の不正利用を防止するため、または情報提供者が自分の提供情報の利用状況を把握するために、記憶部１２のような利用ソフトウェア履歴格納手段を備え、その履歴に基づいて情報提供者が利用者に料金の請求等を行う。「超流通」において情報は買い取りではなくレンタル的な扱いをするために、この利用履歴は必要になるが、このような方式では、利用者がどのような情報を利用したかということが情報提供者に知られてしまい、利用者のプライバシーを保護することができない。

【０００７】（３）「超流通」は提供情報の利用状態を正しく把握する、すなわち、利用料金を正しく把握するための方式ではあるが、料金の支払いに関する手段や方式は含まれていない。このため情報提供者が提供情報の利用状態を知った後は、他の手段によって料金の請求及び徴収を行う必要がある。

【０００８】本発明は上述のような実情に鑑みてなされたものであり、前述の（１）～（３）の問題を解決することのできる課金方式を提供することを目的とする。

【０００９】

【課題を解決するための手段】請求項１の発明による課金装置においては、記録媒体に記録され、所定の金融機関等にて保証された金額を示す金銭情報が入力される入力手段と、上記入力手段から入力された金銭情報を判定し、情報提供者から提供される画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の提供情報の利用を許可する許可信号を出力する判定手段と、上記許可信号に応じて上記提供情報の利用が可能となるように処理する処理手段と、上記金銭情報に関する情報及び上記判定手段による判定の結果を表示する表示手段とを設けている。

【００１０】請求項５の発明による情報受信装置においては、情報提供者から提供される画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の提供情報を受信するように成された情報受信装置であって、所定の金融機関等にて保証された金額を示す金銭情報が入力される入力手段と、上記入力手段から入力された金銭情報を判定して上記提供情報の利用を許可する許可信号を出力する判定手段と、上記許可信号に応じて上記提供情報の利用が可能となるように処理する処理手段と、上記金銭情報に関する情報及び上記判定手段による判定の結果を表示する表示手段とを設けている。

【００１１】請求項１０の発明による通信システムにおいては、情報を提供する情報提供者端末装置と、上記情報提供者端末装置からの画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の提供情報を受信して利用する利用者端末装置と、所定の金融機関等にて保証された金銭情報を入力するように成され、入力された金銭情報を判定して上記提供情報の利用を許可する許可信号を出力する判定手段と上記許可信号に応じて上記提供情報の利用が可能となるように処理する処理手段と上記金銭情報に関する情報及び上記判定手段による判定の結果を表示する表示手段とを有する課金装置とを設けている。

【００１２】

【作用】本発明によれば、現金あるいはプリペイドカード等の記録媒体に記録され、所定の金融機関等にて保証された金銭情報に基づいて判定手段は利用者の画像データ、音声データ、コンピュータデータ、コンピュータプログラム等の提供情報の利用可否を判定し、利用可のとき許可信号を出力し、この許可信号に応じて提供情報の利用が可能となるように処理することにより、利用者は利用者端末等を動作させることで提供情報を得ることができる。また、利用可能な残高等の金銭情報に関する情報を表示するので、利用者はあとどれくらい使用できるのか予め知ることができる。更に、判定の結果を表示することで利用者は自分が欲した情報を利用できるのか否かを直ちに知ることができる。

【００１３】

【発明の実施の形態】以下、本発明に係る第１の実施の形態を図１を参照して説明する。図１において、１０は情報受信装置としての利用者端末、Ｐは情報提供者、Ｐ

Ｐｉ（またはＰＰｊ）は情報提供者Ｐによって有償で提供される提供情報、ＰＩＤｉ（またはＰＩＤｊ）はＰＰｉに付加された固有の情報固有データ、ＰＰＣは後述するように現金やカード等に記録された金銭情報、１４はＰＰＣの入力部、１５は表示部、１６は上記各部１４、１５及び判定部１１を含む課金部、１１は提供情報ＰＰの利用可否を判定する判定部、１７は信号処理部である。

【００１４】次に動作について説明する。情報提供者ＰはＰＩＤを含めた提供情報ＰＰを提供する。利用者端末１０は、その提供情報ＰＰを利用する際には、必ず課金部１６を経由するように構成してある。この課金部１６は金銭情報であるＰＰＣの受け口としての入力部１４がある。提供情報ＰＰの利用要求が生じると、判定部１１はＰＩＤ及び／またはＰＰＣに基づいて、提供情報ＰＰの利用可能性をチェックする。例えば、ＰＩＤに示された利用料金がＰＰＣの金銭情報が示す残高以内か否かなどのチェックである。利用がＯＫ（許可）か否（ＮＧ）かは信号処理部１７に通知され、もしＯＫであれば、信号処理部１７は利用者が提供情報ＰＰの利用が可能となるように処理して出力する。このときのＰＩＤやＰＰＣに関する情報（提供情報の利用料金やＰＰＣの残高など）は表示部１５で表示される。また、判定部１１の利用可否の判定結果も表示部１５で表示することができる。

【００１５】本発明における金銭情報ＰＰＣは実際の金銭（現金）であってもよいし、テレホンカードのようなプリペイドカードであってもよいし、フロッピー（登録商標）ディスク及びＩＣカードやＰＣＭＣＩＡなどに格納された金銭と等価な電子的な情報であっても良い。本発明では、利用者毎の利用者固有データとしてのユーザＩＤを用いず、その代わりに利用者に依存しない金銭情報ＰＰＣによって提供情報ＰＰの利用可否を判定する。従って、利用者はユーザＩＤをもらうための申し込み手続きをする必要が無く、実際の金銭と等価な金銭情報ＰＰＣをもつだけ、即ち利用する情報に対する料金を支払うだけであるので、自然であり容易である。これによって、多くの利用者固有情報を管理する必要もなくなり前記（１）の問題が解決される。

【００１６】また、本発明では利用者固有データを持たないため、利用者は自分がどの情報を利用したかというプライバシーを情報提供者に知られることはない。これは情報提供者Ｐの権利が守られていないように見えるが、自分の提供情報の利用頻度に応じた料金が支払われさえすれば情報提供者Ｐには十分であって、どの利用者かどの情報を利用したかという利用者のプライバシーまで知る必要はない。本発明では、どのユーザＩＤをもつ利用者がどの情報ＰＩＤを利用したかという利用履歴格納手段はもたないが、どの情報が何度利用されたかという利用頻度格納手段または現在提供情報を利用していることを知らせる利用通知手段を有することはできる。図１においては、点線で示す経路によって情報提供者Ｐに利用頻度情報が知らされる。なお、具体的な利用頻度格納手段または利用通知手段については後述する第２～６の実施の形態で詳述する。以上により、前記（２）の利用者のプライバシーの問題も解決される。

【００１７】本発明では、ＰＰＣは金銭と等価な情報であるので、ＰＰＣを用いること自体が料金の支払いに相当する。これによって前記（３）の問題も解決される。なお、具体的なＰＰＣの入手法と回収法、及び料金の分配法は前記（２）の問題と絡めて第２～６の実施の形態に示される。

【００１８】尚、課金部１６は本発明の課金装置であり、これを図１では利用者端末１０の内部に一体的に設けているが、課金部１６を利用者端末１０とは別体に設けてもよい。その場合、情報提供者Ｐから提供情報ＰＰに付加された情報ＰＩＤを課金部１６が先ず受信し、ＰＩＤ、ＰＰＣに基づく判定部１１の判定結果がＯＫであることを示す信号に基づいて利用端末装置１０に対して提供情報ＰＰの受信や信号処理を許可するような構成としてよい。また、このような構成は、後述する第２～第８の実施の形態に適用してよい。

【００１９】次に第２の実施の形態を図２について説明する。図２はＰＰＣが実際の金銭（現金）である場合を示す。この場合のＰＰＣの入力部１４はコインや紙幣の入口であり、利用者はまずこの入力部１４に一定の金銭を入れる。その金銭がＰＩＤに示された料金を超えたときに判定部１１は提供情報ＰＰの利用を許可する。または、課金部１６は表示部１５により利用者に提供情報の利用料金を表示し、利用者はそれに相当する金銭をＰＰＣの入力部１４に入力する。判定部１１はそれをもとに提供情報ＰＰの利用可否を判定する。また、時間に応じて料金が更新される場合には、その旨を表示し、それに応じた追加料金を入力するようにしてもよい。また、入力された金額はコインボックス１８に格納され、情報提供者Ｐまたは料金の回収を行う何らかの機関が回収する。このとき、各提供情報ＰＰ毎の利用頻度はカウンタ１９に記録・回収され、その利用頻度に応じてコインボックス１８の料金が各情報提供者Ｐに分配される。提供情報ＰＰが一つである場合等、利用頻度が必要ない場合にはカウンタ１９は省略できる。

【００２０】次に第３の実施の形態を図３について説明する。図３はＰＰＣがテレホンカードのようなプリペイドカードである場合を示している。利用者はＰＰＣの入力部１４にプリペイドカードをさし込み、それに記載された金額がＰＩＤに示された利用料金（この金額は表示されてもよい）より多いか否かを判定部１１が判定し、多い場合にはＰＰの利用を許可する。この場合、ＰＰの利用料金が時間によって更新されていっても、プリペイドカードの料金内であれば継続して利用可能となるよう

に、判定部１１とＰＰＣの入力１４は構成される。入力部１４がプリペイドカードを追加して挿入できる構成とした場合はさらなる長時間の利用も可能となる。

【００２１】このようなプリペイドカードの入手は現在のテレホンカードと同様に多くの販売店によって市販される販売形態になっていればどこでも容易に入手可能である。この場合、プリペイドカードの製造会社は料金分配者２０となり、情報提供者Ｐはその料金分配者２０に登録することによって提供情報ＰＰの利用頻度に応じた料金の分配を受ける。前述の販売店は料分配者に含まれる。

【００２２】この利用頻度に応じた料金の分配は、課金部１６が通信Ｉ／Ｆ２１を用いて現在の利用情報を料金分配者２０に知らせることによって実現される。この利用通知は課金部１６がプリペイドカードの金額を更新するときに限り出力されるように構成される。提供情報ＰＰを通信によって入力する場合は、この通信Ｉ／Ｆ２１を共有することができる。この場合、図４に示されるように料金分配者２０の端末、情報提供者Ｐの端末及び利用者端末１０はネットワーク２２に接続されており、料金分配者２０は上記通知に応じて料金を情報提供者Ｐに分配する。

【００２３】また、通信Ｉ／Ｆ２１を持たない場合は、利用する情報に応じてプリペイドカードの種類を変えるという方法もある。このとき、判定部１１は情報に応じてプリペイドカードの種類を調べるという処理を行い、それに対する利用可否も判定する。また、課金部１６に提供情報ＰＰの利用記録をプリペイドカードに記録する手段を設け、このプリペイドカードを料金分配者２０が回収することによって、利用頻度に応じた料金の分配を行うこともできる。その場合、プリペイドカードの回収を促進するために、プリペイドカードの交換の場合は、金銭情報のみの料金で済み、プリペイドカードの交換でない場合は、金銭情報の料金の他にプリペイドカード自体の料金も加算されるなどの販売形態にすればよい。ただし、回収できない利用記録に対応する料金は回収できた利用記録に応じた比率で分配しても良い。

【００２４】図５は第４の実施の形態を示すもので、ＰＰＣがフロッピーディスクまたは書き換えが容易な電気的及び／または磁気的なデバイスである場合を示す。また、ネットワークシステムを図６に示す。この場合、ＰＰＣ内に格納される金銭情報は銀行やその他の金融機関等によって保証されたデータであったり、販売店を含む料金分配者２０によってのみ加算処理できる特殊なデータである。利用者は入力部１４にＰＰＣをさし込む。課金部１６はＰＰＣから情報を読み出し、その金額がＰＩＤに示された料金より多く（この金額は表示されてもよい）、課金部１６がＰＰＣに利用料金を請求可能である場合に判定部１１はＰＰの利用を許可（ＯＫ）する。この場合、ＰＰの利用料金が時間によって更新されていっても、ＰＰＣの記載料金以内は継続して利用可能であるように構成される。

【００２５】この場合の金銭情報は電子的な情報であるので、金銭情報の入出力も通信Ｉ／Ｆ２１を介して料金分配者２０との所定の手続きによる通信によって行うことができる。このとき、第１、第２の実施の形態と異り、実際の金銭を利用者は料金分配者２０に直接支払うわけではないので、利用者の金銭支払いを保証するのは利用者と契約を結んだ銀行やその他の金融機関（以後、料金立替者２３）である。さらに、利用情報の通知に関しても、第３の実施の形態と同様に通信Ｉ／Ｆ２１を用いて現在の利用情報を料金分配者２０に知らせることによって、利用頻度に応じた料金の分配が可能になる。この場合、利用料金を電子的な金銭情報ＰＰＣによって直接料金分配者２０や情報提供者Ｐに送ることも可能である。

【００２６】具体的には、次のような通信処理によって電子的な金銭情報の入出力が実現できる。また、課金部１６は後述のような暗号・認証処理手段を有しており、後述するＴＡ等で示されるタイムスタンプを安全に管理する手段を有するものとする。これは、ＰＰＣがフロッピーディスク等の書き換えが容易な媒体であるために、ＰＰＣのコピー等によって不正が行われる可能性があるので、それを防止するためにＰＰＣを認証可能にし、タイムスタンプの管理によってＰＰＣのコピー等の不正に対抗するものである。

【００２７】次に、利用者をＡ、情報提供者をＢ、料金分配者をＣ、料金立替者をＤとし、各々は署名可能な秘密鍵を秘密に保持し、通信相手はその署名を検査できる公開鍵を知っているもの（例えば、Ａの秘密鍵をｓＡ、公開鍵をｐＡとする）として課金処理を説明する。ここで、ＡがＢの提供情報Ｐｉを利用する場合を考える。ただし、Ｘの鍵Ｙによる処理結果を｛Ｘ｝＾Ｙで表し、利用者の各処理及び鍵やタイプスタンプの管理は課金部１６内の安全性が保証された手段または各人の記憶や記録によるものとする。

【００２８】［金銭情報入手処理］

（１）Ａはａ円（通貨の単位は円に限らない）分の金銭情報の入力要求を自分の登録情報ｉＡ（口座番号やクレジット番号など）をつけて秘密鍵ｓＡで署名しＣに送る。

ＭＡ＝｛Ａ，｛Ａ，ｉＡ，ａ，ＴＡ｝＾ｓＡ｝

【００２９】（２）ＣはＭＡの署名をＡの公開鍵ｐＡで検査し、ｉＡを用いてＤにａ円分の請求を行い、それが受け入れられれば金銭情報ａを１円毎または基本単位ｃ毎（情報が１００円単位の価格であれば１００円毎）にＣの署名鍵であるｓＣで署名して次のメッセージをＡに送る。ただし、それらには異なるタイムスタンプＴＣｉがつけられる。

ＭＣ＝Σ｛ＴＡ，｛Ｃ，ｅ，ＴＣｉ｝＾ｓＣ｝＾ｐＡ

【００３０】（３）ＡはＭＣの各々をｐＡで復号し、さらにｓＣに対応するＣの公開鍵ｐＣで署名を検査し、検査結果が正しければ｛Ｃ，ａ，ＴＣｉ｝＾ｓＣをＰＰＣに記録する。なお、ＴＡ、ＴＣｉはタイムスタンプを示すものであり、同じ送信者からの同じタイムスタンプをもつメッセージは不正要求とする。また、ＴＡ、ＴＣｉはシリアル番号や偶然一致することがないまたは少ない乱数のようなものであればタイムスタンプでなくてもよい。

【００３１】［利用情報通知処理］

（１）Ａが情報Ｐｉを利用したいとき、ＡのＰＰＣ内の金銭情報がＰＩＤｉに示された利用料金より大きければ課金部１６はＰｉの利用を許可する。

（２）ＡがＰｉの利用を終了したとき、または利用中に課金部１６はＰＰＣの金銭情報から要した利用料金を消去する。

【００３２】（３）このとき、Ａは次の利用通知ＭＢをＣに送る。ただし、消去された利用料金をｂとする。

ＭＢ＝｛Ａ，Ｂ，｛Ｂ，ｂ，ＴＢ｝＾ｓＡ｝

（４）Ｃはこのメッセージを検査し正しいときに、ｂ円をＢへの分配金として支払う。

【００３３】上記の説明では、処理を簡単にするためにＣと各利用者間の暗号方式は公開鍵暗号としたが、予め鍵が共有されていれば共通鍵暗号を用いてもよいことは明らかである。また、タイムスタンプからの時間によって各メッセージの有効期間を定めることもできる。以上において、メッセージ内の並び順は順不同であり、Ａ、Ｂ等で示す利用者の識別子やタイムスタンプは必ずしも必要でない場合もある。さらに、上記の金銭情報入手処理、利用情報通知処理の手順は１つの例であり、電子的な情報を金銭情報として利用者固有データを用いずに課金処理を行うものは全て本発明に含まれる。

【００３４】また、通信Ｉ／Ｆ２１を持たない場合、利用者は販売店などの料金分配者２０のところでＰＰＣに格納する金銭情報を料金と引き替えに入力してもらう。また、課金部１６が前記ＭＢのような提供情報ＰＰの利用記録をＰＰＣに記録し、ＰＰＣを販売店等の料金分配者２０のところで金銭情報を補充・入力する際に利用記録を補充器が回収することによって、利用頻度に応じた料金の分配を行うようにすることができる。このような電子的な金銭情報は前述したように料金分配者２０だけが処理できる特殊なデータであるので、通信Ｉ／Ｆ２１を持たない利用者はＰＰＣを用いるためには必ず販売店等の料金分配者２０を介する必要があるので、利用記録は必ず回収でき利用頻度に応じた料金の分配が可能である。

【００３５】図７は第５の実施の形態を示すもので、ＰＰＣがＩＣカードやＰＣＭＣＩＡのような電子的なカードである場合を示す。ネットワークシステムの構成は図６と同一である。この場合は、ＰＰＣ内に格納される金銭情報は銀行やその他の金融機関等によって保証されたデータであったり、販売店を含む料金分配者２０によってのみ加算処理できる特殊なデータである。利用者はＰＰＣの入力部１４にＰＰＣをさし込み、所定の手続き（暗証番号の検査など）によってＰＰＣを動作可能にする。課金部１６はＰＰＣから金銭情報を読み出し、その額がＰＩＤに示された料金より多く（金額は表示されてもよい）、課金部１６がＰＰＣに利用料金を請求可能である場合に判定部１１はＰＰの利用を許可する。この場合、ＰＰの利用料金が時間によって更新されていっても、ＰＰＣの記載料金以内は継続して利用可能であるように構成される。

【００３６】この場合の金銭情報は電子的な情報であるので、金銭情報の入出力も通信Ｉ／Ｆ２１を介して料金分配者２０との所定の手続きによる通信により行うことができる。このとき、第１、第２の実施の形態と異り実際の金銭を利用者は料金分配者２０に直接支払うわけではないので、利用者の金銭支払いを保証するのは利用者と契約を結んだ銀行やその他の金融機関、即ち、料金立替者２３である。さらに、利用情報の通知に関しても、第３の実施の形態と同様に通信Ｉ／Ｆ２１を用いて現在の利用情報を料金分配者２０に知らせることによって、利用頻度に応じた料金の分配が可能になる。この場合、利用料金を電子的な金銭情報によって直接料金分配者２０や情報提供者Ｐに送ることも可能である。

【００３７】具体的には、次のような通信処理によって電子的な金銭情報の入出力が実現できる。ただし、通信や処理に関する安全性を考慮してＰＰＣとして用いる電子的なカードはセキュリティ機能として暗証番号による所有者確認や、アクセス条件によるデータメモリへのアクセス制御や、後述のような暗号方式による暗号・認証を行うことができるものとする。このとき、暗号処理や認証処理に用いる秘密鍵は前述のようにアクセス制御されたメモリ領域に書き込まれ、そのアクセス条件を満たす者（カード発行者や料金分配者等）しかアクセスできないものとする。また、以下の課金動作もカードの発行者または料金分配者２０以外変更できない仕様になっているものとする。

【００３８】利用者端末１０、情報提供者Ｐの端末、料金分配者２０の端末、料金立替者２３の端末は図６のようにネットワーク２２で接続されている。ここで、利用者をＡ、情報提供者をＢ、料金分配者をＣ、料金立替者をＤとし、Ｃは各利用者に対して暗号通信のための秘密鍵を共有し（例えば、ＡとＣの間の秘密鍵をｓＡ、ＢとＣの間の秘密鍵をｓＢとする）、Ｃは自分しか知らない署名のための秘密鍵ｓＣを秘密に保持し、それに対応する署名の検査鍵ｐＣを公開しているものとする。以下に、ＡがＢの提供情報Ｐｉを利用する場合を考える。ただし、平文Ｘの鍵Ｙによる暗号文を｛Ｘ｝＾Ｙで表し、利用者の各処理は全て上述のようなセキュリティ機能を

もつＰＰＣ内で行われるものとする。

【００３９】［金銭情報入手処理］

（１）ＡはＣにａ円（通貨の単位は円に限らない）分の金銭情報の入力要求をＤへの自分の登録情報ｉＡ（口座番号やクレジット番号など）をつけてＣに送る。

ＭＡ＝｛Ａ，｛Ａ，ｉＡ，ａ，ＴＡ｝＾ｓＡ｝

【００４０】（２）ＣはＭＡの暗号部分をＡと共有しているｓＡで復号し、ｉＡを用いてＤにａ円分の請求を行い、それが受け入れられれば金銭情報ａにＣの署名鍵であるｓＣで署名して次のメッセージをＡに送る。

ＭＣ＝｛ＴＡ，｛Ｃ，ａ，ＴＣ｝＾ｓＣ｝＾ｓＡ

【００４１】（３）ＡはＭＣをｓＡで復号し、さらにｓＣに対応するＣの公開鍵ｐＣで署名を検査し、検査結果が正しい場合のみＡのＰＰＣはａ円分の金銭情報を加算する。上記ＴＡやＴＣはタイムスタンプであり、同じ送信者からの同じタイムスタンプをもつメッセージは不正要求とする。また、ＴＡ、ＴＣはシリアル番号や偶然一致することがないまたは少ない乱数のようなものであればタイムスタンプでなくてもよい。

【００４２】［利用情報通知処理］

（１）Ａが情報Ｐｉを利用したいとき、ＡのＰＰＣ内の金銭情報がＰＩＤｉに示された利用料金より大きければ課金部１６はＰｉの利用を許可する。

（２）ＡがＰｉの利用を終了したとき、または利用中に課金部１６はＰＰＣの金銭情報から要した利用料金を差し引き、その結果をＰＰＣに書き込む。

【００４３】（３）このとき、Ａは次の利用通知をＣに送る。ただし、差し引いた利用料金をｂとする。

ＭＢ＝｛Ａ，｛Ｂ，ｂ，ＴＢ｝＾ｓＡ｝

（４）Ｃはこのメッセージを復号し正しいときに、ｂ円をＢへの分配金として支払う。

【００４４】次に、ＡとＢの間の情報も暗号通信によってやりとりする場合、次の処理を前述の金銭情報入手処理と利用情報通知処理の間で行えばよい。ただし、Ｃは情報提供者とも秘密鍵を共有しているとする。

【００４５】［情報利用処理］（１）ＡはＣにＢとの会話鍵の生成を依頼するために次のメッセージをＣに送る。

ＭＡ′＝｛Ａ，Ｂ，ＴＡ′｝

（２）Ｃは会話鍵ＣＫを生成し、次のメッセージをＡに送る。

ＭＣ′＝｛｛ＴＣ′，Ａ，ＣＫ｝＾ｓＢ，ＴＡ′，Ｂ，ＣＫ｝＾ｓＡ

【００４６】（３）ＡはＭＣ′をｓＡで復号し、｛ＴＣ′，Ａ，ＣＫ｝＾ｓＢをＢに送る。

（４）Ｂは受信メッセージをｓＢで復号し、会話鍵ＣＫで暗号化した情報をＡに送る。

（５）Ａは会話鍵ＣＫで暗号化情報を復号する。

【００４７】上記の説明では、処理を簡単にするためにＣと各利用者間の暗号方式は共通鍵暗号としたが、第５の実施の形態と同様に公開鍵暗号を用いてもよいことは明らかである。また、タイムスタンプからの時間によって各メッセージの有効期間を定めることもできる。また、メッセージ内の並び順は順不同であり、Ａ、Ｂ等で示す利用者の識別子やタイムスタンプは必ずしも必要でない場合もある。さらに、上記の金銭情報入手処理、利用情報通知処理の手順は１つの例であり、電子的な情報を金銭情報として利用者固有データを用いずに課金処理を行うものは全て本発明に含まれる。

【００４８】また、通信Ｉ／Ｆ２１を持たない場合、利用者は販売店などの料金分配者２０のところでＰＰＣに格納する金銭情報を入力してもらう。また、課金部１６が提供情報ＰＰの利用記録をＰＰＣに記録し、このＰＰＣを販売店等の料金分配者２０のところで金銭情報を補充・入力する際に利用記録を補充器が回収することによって、利用頻度に応じた料金の分配を行うようにすることができる。このような電子的な金銭情報は前述したように料金分配者２０だけが処理できる特殊なデータであるので、通信Ｉ／Ｆ２１を持たない利用者はＰＰＣを用いるためには必ず販売店等の料金分配者２０を介する必要があるので、利用記録は必ず回収でき利用頻度に応じた料金の分配が可能である。

【００４９】図８は第６の実施の形態を示すもので、第５の実施の形態と同様に電子的な情報を金銭情報として用い、料金分配者２０のいらない課金方式を示すものである。利用者端末１０、情報提供者Ｐの端末、料金立替者２３の端末は図９のようにネットワーク２２で接続されている。さらに、ＰＰＣとして用いる電子カードはセキュリティ機能として暗証番号による所有者確認や、アクセス条件によるデータメモリへのアクセス制御や、暗号方式による暗号・認証を行うことができるものとする。このとき、暗号処理や認証処理に用いる秘密の鍵は前述のようにアクセス制御されたメモリ領域に書き込まれているとする。また、以下の課金動作もカードの発行者以外変更できない仕様になっているとする。

【００５０】利用者をＡ、情報提供者をＢ、料金立替者をＤとし、各々は署名可能な秘密鍵を秘密に保持し、通信相手はその署名を検査できる公開鍵を知っているもの（例えば、Ａの秘密鍵をｓＡ、公開鍵をｐＡとする）とする。ここで、ＡがＢの提供情報Ｐｉを利用する場合を考える。ただし、Ｘの鍵Ｙによる処理結果を｛Ｘ｝＾Ｙで表し、利用者の各処理は全て上述のようなセキュリティ機能をもつＰＰＣ内で行われるものとする。

【００５１】［金銭情報入手処理］

（１）Ａはａ円（通貨の単位は円に限らない）分の金銭情報の入力要求を自分の登録情報ｉＡ（口座番号やクレジット番号など）をつけて秘密鍵ｓＡで署名しＤに送る。

ＭＡ＝｛Ａ，｛Ａ，ｉＡ，ａ，ＴＡ｝＾ｓＡ｝

【００５２】（２）ＤはＭＡの署名をＡと公開鍵ｐＡで

検査し、ｉＡが正しくＡがａ円支払可能であれば、金銭情報ａをＤで署名して次のメッセージをＡに送る。

ＭＤ＝｛ＴＡ，｛Ｄ，ａ，ＴＤ｝＾ｓＤ｝＾ｓＡ

【００５３】（３）ＡはＭＤをｐＡで検査し、さらにｓＤに対応するＤの公開鍵ｐＤで署名を検査し、検査結果が正しい場合のみＡのＰＰＣはａ円分の金銭情報を加算する。上記、ＴＡやＴＤはタイムスタンプであり、同じ送信者からの同じタイムスタンプをもつメッセージは不正要求とする。また、ＴＡ、ＴＤはシリアル番号や偶然一致することがない、または少ない乱数のようなものであれば、タイムスタンプでなくてもよい。

【００５４】［利用情報通知処理］

（１）Ａが情報Ｐｉを利用したいとき、ＡのＰＰＣ内の金銭情報がＰＩＤｉに示された利用料金より大きければ課金手段はＰｉの利用を許可する。

（２）ＡがＰｉの利用を終了したとき、または利用中に課金部１６はＰＰＣの金銭情報から要した利用料金を差し引き、その結果をＰＰＣに書き込む。

【００５５】（３）このとき、Ａは次の利用通知ＭＢをＢに送る。ただし、差し引いた利用料金をｂとする。

ＭＢ＝｛Ａ，Ｂ，｛Ｂ，ｂ，ＴＢ｝＾ｓＡ｝

（４）Ｂは署名を検査し正しいときに、Ａの署名｛Ｂ，ｂ，ＴＢ｝＾ｓＡをＤに示し、ｂの料金を受け取る。

【００５６】次に、ＡとＢの間の情報も暗号通信によってやりとりする場合、直接相手の公開鍵で公開鍵による暗号通信を行うこともできるが、情報量が多い場合次のように共通鍵暗号による暗号通信を行うこともできる。この場合、各利用者と情報提供者の間には共通鍵暗号手段が共有されているとする。ただし、下記の（１）、（２）においてＡとＢは逆であっても良い。

【００５７】［情報利用処理］

（１）ＡはＢとの共通鍵ＣＫをＢの公開鍵ｐＢで暗号化して送る。

ＭＡ′＝｛Ａ，Ｂ，ＣＫ，ＴＡ′｝＾ｐＢ

（２）Ｂは受信メッセージをｓＢで復号する。

（３）Ｂは共通鍵ＣＫで共通鍵暗号化した情報をＡに送る。

（４）Ａは共通鍵ＣＫで共通鍵暗号化情報を復号する。

【００５８】上記の説明では、説明を簡単にするためにＤと各利用者と情報提供者Ｐとの暗号方式は公開鍵暗号としたが、前述のような共通鍵暗号を用いてもよいことは明らかである。また、タイムスタンプからの時間によって各メッセージの有効期間を定めることもできる。また、メッセージ内の並び順は順不同であり、Ａ、Ｂ等で示す利用者の識別子やタイムスタンプは必ずしも必要でない場合もある。さらに、上記の金銭情報入手処理、利用情報通知処理の手順は１つの例であり、電子的な情報を金銭情報として利用者固有データを用いずに課金処理を行うものは全て本発明に含まれる。

【００５９】次に、その他の実施の形態を説明する。

第７の実施の形態

第２の実施の形態に示す実際の金銭を用いた課金方式によって、１つ以上の利用者端末１０を設置した施設を情報提供者Ｐまたは料金分配者２０が営業し、公衆電話やゲームセンター、喫茶店、図書館のように多くの人が金銭を支払うことによって自由に利用者端末１０を使用するという課金システムが実現できる。

【００６０】また、第３の実施の形態に示すプリペイドカードを用いた課金方式によって、情報提供者ＰがＣＤ－ＲＯＭやパソコン通信等によって広く提供情報ＰＰを配布し、情報に対する著作権協会のような機関が料金分配者２０となってプリペイドカードを製作・販売し、利用者は販売店などを通じてプリペイドカードを購入し、自宅やその他の端末等で提供情報ＰＰを利用するという課金システムが実現できる。

【００６１】第４の実施の形態に示すフロッピーディスクを用いた課金方式によって、第３の実施の形態におけるＰＰＣのための特殊な入力部１４を必要とせず（利用者端末には通常フロッピーディスクの入力部１４はついているとする）、さらに金銭情報の通信によるやりとりによって販売店を省略可能とし、暗号・認証処理をソフト的に行うことによって現在のネットワークで容易に実現可能な課金システムが構成できる。

【００６２】第５の実施の形態に示すＩＣカードやＰＣＭＣＩＡ等の電子的なカードを用いた課金方式によって、上記第４の実施の形態を用いた課金システムをより安全にした課金システムが実現できる。第６の実施の形態に示す課金方式によって、料金分配者２０のいらない、即ち利用者と情報提供者Ｐとが料金立替者２３を通して直接取引をする課金システムが実現できる。また、この課金方式及び課金システムは将来実用化されると思われるある特殊なデータを金銭と同様に扱う電子現金に対しても適用可能であることは明らかである。さらに、上記の課金方式、及び課金システムを組み合わせた種々の課金システムも本発明に含まれる。

【００６３】第８の実施の形態

現在、情報提供者が多くの情報を異なる鍵で暗号化してＣＤ－ＲＯＭ等に納め、媒体としてのＣＤ－ＲＯＭ自体は販売店を通じて安価に販売し、利用者からの依頼に応じて情報提供者が利用者に指定情報の暗号鍵を知らせるときにその情報の利用対価を請求する課金方式が知られている。しかし、この方式ではＣＤ－ＲＯＭを販売する販売店は媒体としての販売利益は得られても、提供情報を販売したことに対する利益は得られないと言う問題がある。

【００６４】そこで、本発明で示したＰＰＣによる課金方式をレンタル的な情報の利用ではなく、情報の買い取りに対して用いることによって上記の問題が解決できる。即ち、利用者は販売店でのＣＤ－ＲＯＭ購入と同時に、プリペイドカード等のＰＰＣも購入し、情報提供者

との通信（電話など）によって暗号鍵を知るときにプリペイドカードでの支払を指定することによって、情報提供者はそのプリペイドカードを販売した販売店から利用料金を回収する。これによって、情報の利用料金の流れに対しても販売店を経由するので、販売店は情報利用に対する利益も得ることができる。その場合、課金部１６はＰＰＣの金銭情報を検査し、情報の利用が可能であれば、情報に対する暗号化を復号するときだけＰＰＣから料金を引くように構成する。さらに、このＰＰＣは使用しないときには換金できるとする。このとき、ＰＰＣは情報提供者毎に製作され、販売店を通じてＣＤ－ＲＯＭと同様に販売される。従って、この実施の形態では料金分配者２０は必要としない。

【００６５】また、第３の実施の形態において利用情報通知処理を以下のようにすることで、プリペイドカードの利用情報通知処理も安全にすることができる。ただし、プリペイドカードにはプリペイドカード毎の識別番号ｉＰとそれに対応した秘密鍵ｓＰとが登録されているものとする。

【００６６】［利用情報通知処理］

（１）ＡのＰＰＣ内の金銭情報がＰＩＤｉに示された利用料金より大きければＣＨＥＣＫは情報Ｐｉの利用を許可する。

（２）ＡがＰｉの利用を終了したとき、または利用中にＣＨＥＣＫはＰＰＣの金銭情報から要した利用料金を差し引き、その結果をＰＰＣに書き込む。

【００６７】（３）このとき、ＣＨＥＣＫは次の利用通知をＣに送る。ただし、Ｂへの利用料金をｂとする。

ＭＢ＝｛ｉＰ，｛Ｂ，ｂ，ｉＰ，ＴＢ｝＾ｓＰ｝

（４）ＣはＭＢを登録した秘密鍵ｓＰで復号し、このメッセージが正しいときにｂ円をＢへ分配金として支払う。これによって、ｉＰとｓＰを知るもの以外、利用通知を生成することはできない。

【００６８】次に、共通鍵暗号方式及び公開鍵暗号方式について説明する。

［共通鍵暗号方式］共通鍵暗号方式は送信者と受信者で同一の暗号鍵を秘密に共有する暗号方式（秘密鍵暗号方式、対称暗号方式、慣用暗号方式とも呼ばれる）である。共通鍵暗号方式は、適当な長さの文字列（ブロック）ごとに同じ鍵で暗号化するブロック暗号と文字列またはビットごとに鍵を変えていくストリーム暗号に分けることができる。ブロック暗号には文字の順序を置き換えて暗号化する転置式暗号や、文字を他の文字に置き換える換字式暗号等がある。この場合、転置や換字の対応表が暗号鍵となる。

【００６９】ストリーム暗号には多表を用いるビジネル暗号や１回限りの使い捨ての鍵を用いるバーナム暗号等が知られている（各暗号の詳細は池野、小山著「現代暗号理論」電子情報通信学会、１９８６．の第２章及び第４章参照）。また、ブロック暗号のなかでもアルゴリズムが公開されているＤＥＳ（Ｄａｔａ Ｅｎｃｒｙｐｔｉｏｎ Ｓｔａｎｄａｒｄ）やＦＥＬＡ（Ｆａｓｔ ｄａｔａ Ｅｎｃｉｐｈｅｒｍｅｎｔ ＡＬｇｏｒｉｔｈｍ）といった暗号（詳細は辻井、笠原著「暗号と情報セキュリティ」昭晃堂、１９９０．の第２章参照）が商用暗号として広く用いられている。

【００７０】ただし、ＤＥＳやＦＥＬＡはアルゴリズムを公開しているために暗号解読法も開発され、その解読法に対抗するために種々の変形が行われていることがある（例えば、後述の繰り返し回数を増したり（Ｃ．Ｈ．Ｍａｙｅｒ ａｎｄ Ｓ．Ｍ．Ｍａｔｙａｓ：“ＣＲＹＰＴＯＧＲＡＰＨＹ－Ａ Ｎｅｗ Ｄｉｍｅｎｓｉｏｎ ｉｎ Ｃｏｍｐｕｔｅｒ Ｄａｔａ Ｓｅｃｕｒｉｔｙ”，Ｗｉｌｅｙ－Ｉｎｔｅｒｓｃｉｃｎｃｅ，Ａｐｐｃｎｄｉｘ Ｄ，ｐｐ．６７９－７１２，１９８２参照）、鍵を頻繁に変える（山本、岩村、松本、今井：“２乗型疑似乱数生成器とブロック暗号を用いた実用的暗号方式”，信学技報，ＩＳＥＣ９３－２９，ｐｐ．６５－７５，１９９３．参照）などの変形が提案されている）。

【００７１】［公開鍵暗号方式］公開鍵暗号方式は暗号鍵と復号鍵が異なり、暗号鍵を公開、復号鍵を秘密に保持する暗号方式である。以下公開鍵暗号について（ａ）で特徴、（ｂ）でプロトコル、（ｃ）で代表例、（ｄ）で具体的な方式としてＲＳＡ暗号についてそれぞれ述べる。

【００７２】（ａ）公開鍵暗号の特徴

（１）暗号鍵と復号鍵とが異なり暗号鍵を公開できるため、暗号鍵を秘密に配送する必要がなく、鍵配送が容易である。

（２）各利用者の暗号鍵は公開されているので、利用者は各自の復号鍵のみ秘密に記憶しておけばよい。

（３）送られてきた通信文の送信者が偽物でないこと及びその通信文が改ざんされていないことを受信者が確認するための認証機能を実現できる。

【００７３】（ｂ）公開鍵暗号のプロトコル

通信文Ｍに対して、公開の暗号鍵Ｋｐを用いた暗号化操作をＥ（ｋｐ，Ｍ）とし、秘密の復号鍵ｋｓを用いた復号操作をＤ（ｋｓ，Ｍ）とすると、公開鍵暗号アルゴリズムは、まず次の２つの条件を満たす。

【００７４】（１）ｋｐが与えられたとき、Ｅ（ｋｐ，Ｍ）の計算は容易である。ｋｓが与えられたとき、Ｄ（ｋｓ，Ｍ）の計算は容易である。

（２）もし、ｋｓを知らないなら、ｋｐとＥの計算手順と　Ｃ＝Ｅ（ｋｐ，Ｍ）を知っていても、Ｍを決定することは計算量の点で困難である。次に、上記（１）、（２）に加えて、次の（３）の条件が成立することにより秘密通信が実現できる。

【００７５】（３）全ての通信文（平文）Ｍに対し、Ｅ（ｋｐ，Ｍ）が定義でき、Ｄ（ｋｓ，Ｅ（ｋｐ，Ｍ））

＝Mが成立する。つまり、ｋｐは公開されているため誰もがＥ（ｋｐ，Ｍ）を計算することができるが、Ｄ（ｋｓ，Ｅ（ｋｐ，Ｍ））を計算してMを得ることができるのは秘密鍵ｋｓを持っている本人だけである。一方、上記（１）、（２）に加えて、次の（４）の条件が成立することにより認証通信が実現できる。

【００７６】（４）すべての通信文（平文）Mに対し、Ｄ（ｋｓ，Ｍ）が定義でき、Ｅ（ｋｐ，Ｄ（ｋｓ，Ｍ））＝Mが成立する。つまり、Ｄ（ｋｓ，Ｍ）を計算できるのは秘密鍵ｋｓを持っている本人のみであり、他の人が偽の秘密鍵ｋｓ′を用いてＤ（ｋｓ′，Ｍ）を計算し、ｋｓを持っている本人になりすましたとしても、Ｅ（ｋｐ，Ｄ（ｋｓ′，Ｍ））≠Mなので受信者は受けとった情報が不正なものであることを確認できる。また、Ｄ（ｋｓ，Ｍ）が改ざんされてもＥ（ｋｐ，Ｄ（ｋｓ，Ｍ）′）≠Mとなり、受信者は受けとった情報が不正なものであることを確認できる。

【００７７】公開鍵暗号では、公開鍵を用いる処理Ｅを暗号化、秘密鍵を用いる処理Ｄを復号と呼んでいる。従って、秘密通信では送信者が暗号化を行い、その後受信者が復号を行うが、認証通信では送信者が復号を行い、その後受信者が暗号化を行うことになる。

【００７８】以下に公開鍵暗号により送信者Ａから受信者Ｂへ秘密通信、認証通信、署名付秘密通信を行う場合のプロトコルを示す。Ａの秘密鍵をｋｓＡ、公開鍵をｋｐＡとし、Ｂの秘密鍵をｋｓＢ、公開鍵をｋｐＢとする。

【００７９】［秘密通信］ＡからＢへの通信文（平文）Mを秘密通信する場合次の手順で行う。Ｓｔｅｐ１：ＡはＢの公開鍵ｋｐＢでMを暗号化し、暗号文ＣをＢに送る。

Ｃ＝Ｅ（ｋｐＢ，Ｍ）

Ｓｔｅｐ２：Ｂは自分の秘密鍵ｋｓＢでＣを復号し、もとの平文Mを得る。

Ｈ＝Ｄ（ｋｓＢ，Ｃ）

受信者Ｂの公開鍵は不特定多数に公開されているので、Ａに限らず全ての人がＢに秘密通信できる。

【００８０】［認証通信］ＡからＢへの通信文（平文）Mを認証通信する場合次の手順で行う。Ｓｔｅｐ１：Ａは自分の秘密鍵ｋｓＡで送信文Ｓを生成しＢに送る。

Ｓ＝Ｄ（ｋｓＡ，Ｍ）

この送信文Ｓを署名文といい、署名文を得る操作を署名という。Ｓｔｅｐ２：ＢはＡの公開鍵ｋｐＡでＳを復元変換し、もとの平文Mを得る。

Ｍ＝Ｅ（ｋｐＡ，Ｓ）

もしMが意味のある文であることを確認したならば、Mが確かにＡから送られてきたことを認証する。送信者Ａの公開鍵は不特定多数に公開されているので、Ｂに限らず全ての人がＡの署名文を認証できる。このような認証をディジタル署名ともいう。

【００８１】［署名付秘密通信］ＡからＢへの通信文（平文）Mを署名付秘密通信する場合次の手順で行う。

Ｓｔｅｐ１：Ａは自分の秘密鍵ｋｓＡでMを署名し、署名文Ｓを作る。

Ｓ＝Ｄ（ｋｐＡ，Ｍ）

さらにＡはＢの公開鍵ｋｐＢでＳを暗号化し、暗号文ＣをＢに送る。

Ｃ＝Ｅ（ｋｐＢ，Ｓ）

Ｓｔｅｐ２：Ｂは自分の秘密鍵ｋｓＢでＣを復号し、署名文Ｓを得る。

Ｓ＝Ｄ（ｋｓＢ，Ｃ）

さらに、ＢはＡの公開鍵ｋｐＡでＳを復元変換し、もとの平文Mを得る。

Ｍ＝Ｅ（ｋｐＡ，Ｓ）

もし、Mが意味のある文であることを確認したならば、Mが確かにＡから送られてきたことを認証する。

【００８２】なお、署名付秘密通信の各Ｓｔｅｐ内における関数を施す順序はそれぞれ逆転してもよい。すなわち、上記の手順では、

Ｓｔｅｐ１：Ｃ＝Ｅ（ｋｐＢ，Ｄ（ｋｓＡ，Ｍ））

Ｓｔｅｐ２：Ｍ－Ｅ（ｋｐＡ，Ｄ（ｋｓＢ，Ｃ））

となっているが、下記のような手順でも署名付秘密通信が実現できる。

Ｓｔｅｐ１：Ｃ＝Ｄ（ｋｓＡ，Ｅ（ｋｐＢ，Ｍ））

Ｓｔｅｐ２：Ｍ＝Ｄ（ｋｓＢ，Ｅ（ｋｐＡ，Ｃ））

（ｃ）代表的な公開鍵暗号方式

【００８３】次に代表的な公開鍵暗号方式の例を以下に挙げる。秘密通信と認証通信ができる方式として

・ＲＳＡ暗号（Ｒ．Ｌ．Ｒｉｖｅｓｔ，Ａ．Ｓｈａｍｉｒ ａｎｄ Ｉ．Ａｄｌｅｍａｎ：“Ａ ｍｅｔｈｏｄ ｏｆ ｏｂｔａｉｎｉｎｇ ｄｉｇｉｔａｌｓｉｇｎａｔｕｒｅｓ ａｎｄ ｐｕｂｌｉｃ ｋｅｙ ｃｒｙｐｔｏｓｙｔｅｍｓ”，Ｃｏｍｍ．ｏｆ ＡＣＭ，１９７８），

・Ｒ暗号（Ｍ．Ｒａｂｉｎ：“Ｄｉｇｉｔａｌｉｚｅｄ ｓｉｇｎａｔｕｒｅｓ ａｎｄ ｐｕｂｌｉｃ－ｋｅｙ ｃｒｙｐｔｏｓｙｓｔｅｍｓ”，ＭＩＴ／ＬＣＳ／ＴＲ－２１２，Ｔｅｃｈｎｉｃａｌ Ｒｅｐｏｒｔ ＭＩＴ．１９７９），

・Ｗ暗号（Ｈ．Ｃ．Ｗｉｌｌｉａｍｇ：“Ａ ｍｏｄｉｆｉｃａｔｉｏｎ ｏｆ ｔｈｅ ＲＳＡ ｐｕｂｌｉｃ－ｋｅｙ ｅｎｃｒｙｐｔｉｏｎ ｐｒｏｃｅｄｎｒｅ”，ＩＥＥＥ Ｔｒａｎｓ ｆｎｆ．Ｔｈｅｏｒｙ，ＩＴ－２６．６，１９８０），

・ＭＩ暗号（松本、今井：“公開鍵暗号系の新しいアルゴリズム”，信学技報，ＩＴ８２－８４，１９８２：Ｔ．Ｍａｔｓｕｍｏｔｏ ａｎｄ Ｈ．Ｉｍａｉ：“Ａ ｃｌａｓｓ ｏｆ ａｓｙｍｍｅｔｒｉｃ ｃｒｙｐｔｏｓｙｓｔｅｍｓ ｂａｓｅｄ ｏｎ ｐｏｌｙｎｏｍｉａｌｓ ｏｖｅｒ ｆｉｎｉｔｅ ｒｉｎｇｓ”，

IEEE International Symp. on Information Theory, 1983)、

【００８４】秘密通信のみができる方式として

・MH暗号(R. C. Merkle and M. E. Hellman: "Hiding information and sjgnatures intrapdoor knapsacks", IEEE Trnas. Inf. Theory, IT－24, 5, 1978)、

・GS暗号(A. Shamir and R. E. Zippel; "On the security of the Merkle-Hellman cryptographic scheme", IEEE Trans Inf. Theory, IT－26, 3, 1980)、

・CR暗号(B. Chor and R. L. Rivest: "A knapsack type public key cryptosystem based on arithmetric in finite field", Proc Crypto 84)、

・M暗号(R. J. McElioce: "A public－key cryptosystem based on algcbraic codingtheory" DSN Progress Rep, Jet Propulsion Lab 1978)、

・E暗号(T. E. ElCamal: "A public key cryptosystem and a signature scheme based on discretre logarithm", Proc Crypto 84, 1984)、

・T暗号(辻井重男, "行列分解を利用した公開鍵暗号の一方式", 信学技報, IT8512, 1985)、

【００８５】認証通信のみできる方式として

・S暗号(A. Shamir: "A fast signature scheme", Report MIT／LCS／TM－107, MIT laboratory for computer science Cambridge, Mass, 1978)、

・L暗号(K. Lieberherr: "Uniform complcxity and digital signaturc" Lecture Notes in Computer Science 115 AutomataLanguage and Programming, Eighth Colloquium Acre, Israel, 1981)、

・GMY暗号(S. Goldwasser. S. Micali and A. Yao: "Strong signature schemes", ACM Symp. on Theory of Computing, 1983)、

・GMR暗号(S. Goldwasser, S. Micali and R. L. Rivest: "A" paradoxical "solution tothe signature problem", ACM Symp. on Foundation of Computer Science, 1984)、

・OSS暗号(H. Ong, C. P. Schnorr and A Shamir: "An efficient signature scheme based on quadratic equation", ACM Symp. on Theory of Computing, 1984)、

・OS暗号(岡本、白石："多項式演算によるディジタル署名方式", 信学論(D), J86－D, 5, 1985：T. Okamoto and A. Shiraisi: "A fast signature scheme basedon quadratic inequalities" IEEE Symp. on Thcory of Computing, 1984)

などをはじめ様々な方式が提案されている。

【００８６】

【発明の効果】以上説明したように、本発明によれば、マルチメディアネットワーク等における前述した(１)～(３)に示した従来の問題を解決した課金方式及び課金システムが実現できる。これによって、利用者は種々の情報をレンタル的に安価に利用しながらプライバシーの保護ができ、情報提供者は利用者毎の情報利用の管理を行うことなく、提供情報の利用頻度に応じて利用料金の分配を受けることができる。また、販売店を含む料金分配者や料金立替者を導入することによって、料金の支払いまで含めて使い勝手の良い課金システムを構成することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態を示すブロック図である。

【図２】本発明の第２の実施の形態を示すブロック図である。

【図３】本発明の第３の実施の形態を示すブロック図である。

【図４】第３の実施の形態によるネットワークのブロック図である。

【図５】本発明の第４の実施の形態を示すブロック図である。

【図６】第４、第５の実施の形態によるネットワークのブロック図である。

【図７】本発明の第５の実施の形態を示すブロック図である。

【図８】本発明の第６の実施の形態を示すブロック図である。

21　　22

【図９】第６の実施の形態によるネットワークのブロック図である。

【図１０】従来の超流通方式を説明するためのブロック図である。

【符号の説明】

Ｐ　情報提供者

ＰＰＣ　金銭情報

１０　利用者端末

＊１１　判定部

１４　ＰＰＣ入力部

１６　課金部

１７　信号処理部

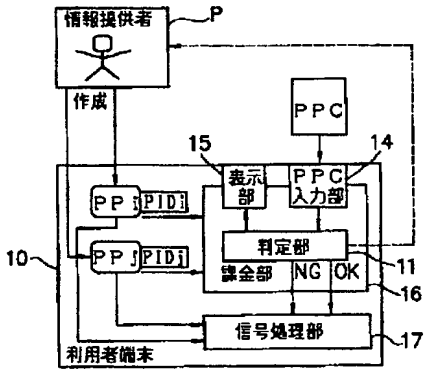
２０　料金分配者

２１　通信Ｉ／Ｆ

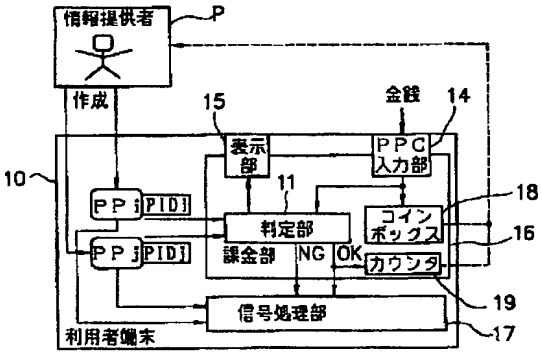
２２　ネットワーク

＊　２３　料金立替者

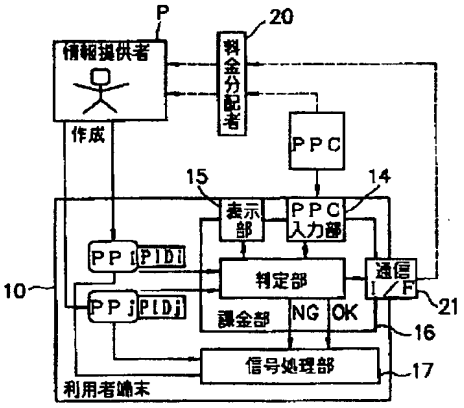
【図１】



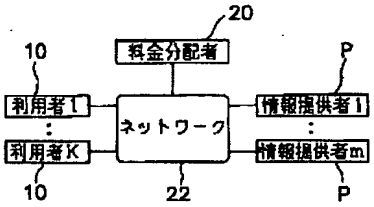
【図２】



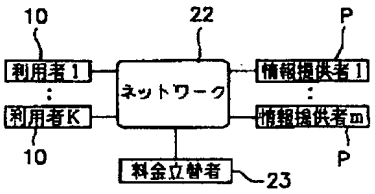
【図３】



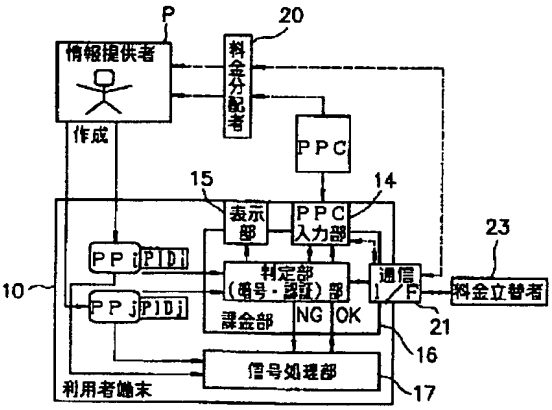
【図４】



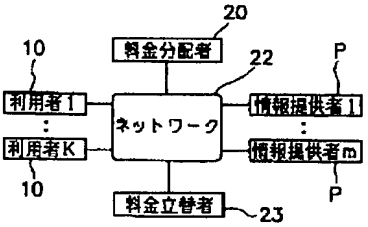
【図９】



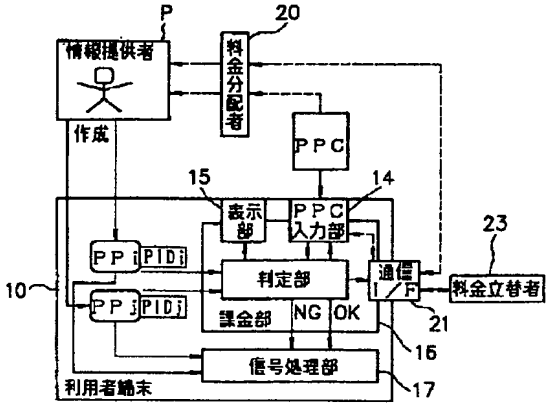
【図５】



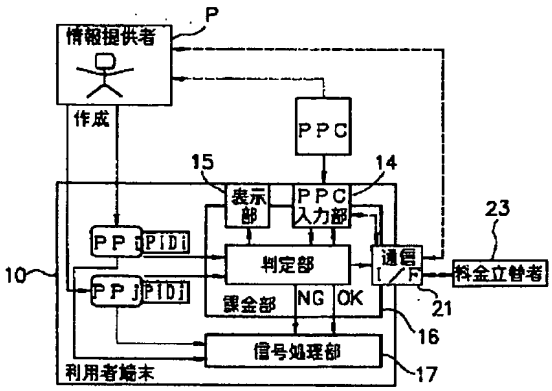
【図６】



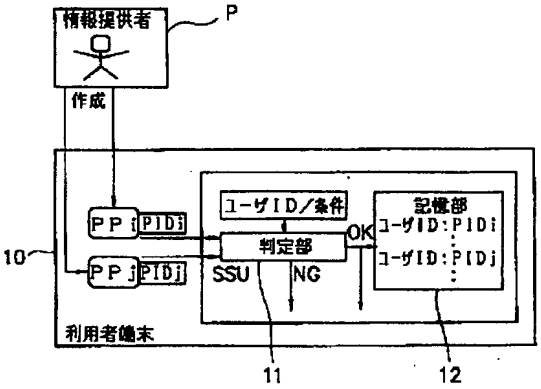
【図７】



【図８】



【図１０】



フロントページの続き

(51)Int.Cl.'	識別記号	FI		テーマコード(参考)
G06F 17/60	510	G06F 17/60	510	
G06K 17/00		G06K 17/00	R	
G07F 17/00		G07F 17/00	B	